ABSTRACT

Systems and methods for preventing a Man-in-the-Middle attack on a communications network, without combining encryption keys of an inner authentication protocol and a tunneling protocol encapsulating the inner authentication protocol. The performance of a hash function may be split between two network devices on the communications network. For example, in response to a challenge issued by a tunnel server, a client may initiate performance of a hash function using only a first part only of the challenge and generate an intermediate result of the hash function (i.e., a preliminary hash). The client then may transmit the preliminary hash to the tunnel server as part of a response to the challenge. The tunnel server then may complete the hash function using the preliminary hash and the remaining part of the challenge to produce a final hash. The final hash then may be used to authenticate a user.